UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/720,087	11/25/2003	Yoshiharu Maeda	1081.1185	4918

21171 7590 08/18/2008
STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
DESIR, PIERRE LOUIS	

ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
08/18/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/720,087	MAEDA ET AL.	
	Examiner	Art Unit	
	PIERRE-LOUIS DESIR	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 1-23 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-2, 5, 16-20, and 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Giniger (previously disclosed) in view of Tatebayashi et al. (Tatebayashi), US 6009174.

Regarding claim 1, Giniger discloses a system comprising a terminal for measuring the position of the mobile body (i.e., means for determining present position information from received position signals) (see col. 5, lines 52-53), encrypting the measured position information by predetermined encryption means and transmitting the encrypted position information (i.e., means for encrypting the present position information and means coupled to the encrypting means for sending the encrypted present position information to the central server) (see col. 6, lines 21-26); and a position recording apparatus (i.e., central server) (see col. 5, lines 50-51), remotely located from the terminal (see fig. 1), communicating with the terminal through a radio network (i.e., wireless means for establishing a bidirectional communications) (see col. 5, lines

51-58), receiving the encrypted position information transmitted from the terminal through a radio network (i.e., means for receiving the present position information from the mobile unit via the bidirectional communications link) (see col. 5, line 66 to col. 6, line 1) and recording the encrypted position information in an encrypted state (i.e., by receiving the present position information, the central site server inherently records or stores the present position information to compare it with stored responses information) (see col. 5, line 66 to col. 6, line 7).

Giniger also discloses a system wherein the position recording apparatus can decrypt the recorded encrypted position information only after the terminal sends the decryption data to allow the position recording apparatus to decrypt the encrypted position information and the position recording apparatus receives the decryption data from the terminal (i.e., means, coupled to the encrypted present position information receiving means, for decrypting the encrypted present position information) (see col. 6, lines 35-37). Also, Ginger discloses in col. 17, lines 29-57.

It should be noted that Giniger discloses a system wherein, for performing security functions, the security element utilizes an authentication and key exchange protocol, and includes, private key, public key crypto algorithm, public key certificate, symmetric key crypto algorithm (see col. 15, lines 12-18).

Giniger, however, does not specifically disclose a system wherein the recording apparatus can decrypt the previously recorded encrypted position information only after the terminal sends a key used to decrypt the previously recorded encrypted position information and that the recording apparatus receives the key from the terminal.

However, Tatebayashi discloses a system a transmission apparatus includes a secret key storage unit that stores three secret keys, a secret key selection unit that selects one secret key from the secret keys, a message generation unit for generating a message M used as a carrier for indicating a secret key, an encryption module for generating a cryptogram by encrypting the generated message using the secret key, an encryption module for generating a cryptogram by encrypting the message using the message itself as the secret key, and two transmission units for transmitting the cryptograms to the reception apparatus to indicate the selected secret key. The reception apparatus includes a decryption module for generating decrypted data by decrypting the cryptogram using a secret key out of the three secret keys, and a decryption module for generating decrypted data by decrypting the cryptogram using the decrypted data, and authorizes that the secret key has been selected when the decrypted data matches the decrypted data (see abstract, col. 1, line 50-col. 2, line 11).

As can be read above, a transmission apparatus transmits a secret key to a reception apparatus. The secret key is used to decrypt or decipher. Combining the teachings of Tatebayashi with the teachings of Giniger would result in a system wherein location information is measured, encrypted, and sent to a server. Using a secret key sent by the terminal, i.e., transmission apparatus, to the server, i.e., reception apparatus, the server decrypt the information.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by Giniger with the teachings described by Tatebayashi to arrive at the claimed invention. A motivation for doing so would have been to provide secure access to information by maintaining the integrity and confidentiality of the information.

Regarding claim 2, Giniger discloses a system (see claim 1 rejection) wherein the position recording apparatus transmits to the terminal the encrypted position information of the mobile body, which was recorded at the position recording apparatus, corresponding to the terminal, based on a request from the terminal (i.e., means for sending an encrypted retrieved response information to the mobile unit) (see col. 6, lines 37-43), and wherein the terminal decrypts the received encrypted position information using the decryption key that the terminal retains (i.e., the mobile unit's means for receiving response information comprises means for decrypting the encrypted response information) (see col. 6, lines 26-31). Also refer to col. 17, lines 29-57. Although one skilled in the art would unhesitatingly conceptualize that the decryption means used by the terminal to decrypt the received location information is a key, Giniger does not specifically disclose terminal sending a decryption key to a position recording apparatus, i.e., server.

However, Tatebayashi discloses a system wherein a transmission apparatus transmits a secret key (i.e., decryption key) to a receiving apparatus to decrypt received message (see abstract, col. 1, line 50-col. 2, line 11).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by Giniger with the teachings described by Tatebayashi to arrive at the claimed invention. A motivation for doing so would have been to provide secure access to information by maintaining the integrity and confidentiality of the information.

Regarding claim 5, Giniger discloses a system (see claim 1 rejection) wherein after the position recording apparatus has received the decryption data retained by the terminal from the

terminal, the position recording apparatus, based on a request from the terminal, decrypts the encrypted position information of a mobile body corresponding to the terminal using the decryption data information (i.e., means, coupled to the encrypted present position information receiving means, for decrypting the encrypted present position information) (see col. 6, lines 35-37. Also refer to col. 17, lines 29-57), executes a predetermined process for the decrypted position information and transmits the result of the process to the terminal (i.e., means for sending an encrypted retrieved response information to the mobile unit) (see col. 6, lines 37-43).

Although Giniger discloses a system as described, Giniger does not specifically disclose a system wherein the server, i.e., position recording apparatus, receives a key from the terminal.

However, Tatebayashi discloses a system wherein a transmission apparatus transmits a secret key (i.e., decryption key) to a receiving apparatus to decrypt received message (see abstract, col. 1, line 50-col. 2, line 11).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by Giniger with the teachings described by Tatebayashi to arrive at the claimed invention. A motivation for doing so would have been to provide secure access to information by maintaining the integrity and confidentiality of the information.

Regarding claim 16, Giniger discloses a terminal comprising a measuring unit for measuring the position of a mobile body i.e., means for determining present position information from received position signals) (see col. 5, lines 52-53); an encryption unit for encrypting the measured position information by predetermined encryption means (i.e., means for encrypting the present position information and means coupled to the encrypting means for sending the

encrypted present position information to the central server) (see col. 6, lines 21-26); a communication unit for transmitting the encrypted position information to a position recording apparatus that records the encrypted position information, remotely located from the terminal, from the terminal through a radio network (e.g., bidirectional communications link) (see col. 5, line 66 to col. 6, line 1) (i.e., means coupled to the encrypting means for sending the encrypted present position information to the central server) (see col. 6, lines 21-26); and decryption unit having decryption data for decrypting the recorded encrypted position information after receiving the encrypted position information from the communication unit, wherein the terminal sends the decryption data to the position recording apparatus only after the terminal allows the position recording apparatus to decrypt the recorded encrypted position information (i.e., means, coupled to the encrypted present position information receiving means, for decrypting the encrypted present position information) (see col. 6, lines 35-37. Also refer to col. 17, lines 29-57).

Giniger also discloses a system wherein the position recording apparatus (i.e., server) can decrypt the recorded encrypted position information only after the terminal sends the decryption data to allow the position recording apparatus to decrypt the encrypted position information and the position recording apparatus receives the decryption data from the terminal (i.e., means, coupled to the encrypted present position information receiving means, for decrypting the encrypted present position information) (see col. 6, lines 35-37). Also, Ginger discloses in col. 17, lines 29-57.

It should be noted that Giniger discloses a system wherein, for performing security functions, the security element utilizes an authentication and key exchange protocol, and

includes, private key, public key crypto algorithm, public key certificate, symmetric key crypto algorithm (see col. 15, lines 12-18).

Giniger, however, does not specifically disclose a terminal wherein the recording apparatus can decrypt the encrypted position information only after the terminal sends a key used to decrypt the encrypted position information and that the recording apparatus receives the key from the terminal.

However, Tatebayashi discloses a system a transmission apparatus includes a secret key storage unit that stores three secret keys, a secret key selection unit that selects one secret key from the secret keys, a message generation unit for generating a message M used as a carrier for indicating a secret key, an encryption module for generating a cryptogram by encrypting the generated message using the secret key, an encryption module for generating a cryptogram by encrypting the message using the message itself as the secret key, and two transmission units for transmitting the cryptograms to the reception apparatus to indicate the selected secret key. The reception apparatus includes a decryption module for generating decrypted data by decrypting the cryptogram using a secret key out of the three secret keys, and a decryption module for generating decrypted data by decrypting the cryptogram using the decrypted data, and authorizes that the secret key has been selected when the decrypted data matches the decrypted data (see abstract, col. 1, line 50-col. 2, line 11).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by Giniger with the teachings described by Tatebayashi to arrive at the claimed invention. A motivation for doing so would have been to

provide secure access to information by maintaining the integrity and confidentiality of the information.

Regarding claim 17, Giniger discloses position recording apparatus remotely located from a terminal of a mobile body (i.e., central site server) (see fig. 1), the position recording apparatus comprising: a communication for receiving encrypted position information relating to the position of at least one mobile body, from a terminal of the mobile body (i.e., means coupled to the encrypting means for sending the encrypted present position information to the central server) (see col. 6, lines 21-26); and a database (i.e., inherently part of the central server site) in which the position information is recorded in the encrypted state (see col. 6, lines 1-7, 19-43), wherein the position recording apparatus can decrypt the recorded encrypted position information only after the terminal sends decryption data to allow the position recording apparatus to decrypt the recorded encrypted position information and the position recording apparatus receives the decryption data from the terminal (i.e., means, coupled to the encrypted present position information receiving means, for decrypting the encrypted present position information) (see col. 6, lines 35-37. Also refer to col. 17, lines 29-57).

Giniger also discloses a system wherein the position recording apparatus (i.e., server) can decrypt the recorded encrypted position information only after the terminal sends the decryption data to allow the position recording apparatus to decrypt the encrypted position information and the position recording apparatus receives the decryption data from the terminal (i.e., means, coupled to the encrypted present position information receiving means, for decrypting the encrypted present position information) (see col. 6, lines 35-37). Also, Ginger discloses in col. 17, lines 29-57.

It should be noted that Giniger discloses a system wherein, for performing security functions, the security element utilizes an authentication and key exchange protocol, and includes, private key, public key crypto algorithm, public key certificate, symmetric key crypto algorithm (see col. 15, lines 12-18).

Giniger, however, does not specifically disclose a position recording apparatus wherein the recording apparatus can decrypt the encrypted position information only after the terminal sends a key used to decrypt the encrypted position information and that the recording apparatus receives the key from the terminal.

However, Tatebayashi discloses a system a transmission apparatus includes a secret key storage unit that stores three secret keys, a secret key selection unit that selects one secret key from the secret keys, a message generation unit for generating a message M used as a carrier for indicating a secret key, an encryption module for generating a cryptogram by encrypting the generated message using the secret key, an encryption module for generating a cryptogram by encrypting the message using the message itself as the secret key, and two transmission units for transmitting the cryptograms to the reception apparatus to indicate the selected secret key. The reception apparatus includes a decryption module for generating decrypted data by decrypting the cryptogram using a secret key out of the three secret keys, and a decryption module for generating decrypted data by decrypting the cryptogram using the decrypted data, and authorizes that the secret key has been selected when the decrypted data matches the decrypted data (see abstract, col. 1, line 50-col. 2, line 11).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by Giniger with the teachings described by

Tatebayashi to arrive at the claimed invention. A motivation for doing so would have been to provide secure access to information by maintaining the integrity and confidentiality of the information.

Regarding claim 18, Giniger discloses an apparatus (see claim 17 rejection) further comprising: an acquisition unit for acquiring the position information recorded in the database, in response to a predetermined request (i.e., means for determining present position information from received position signals) (see col. 5, lines 52-53), wherein the communication unit transmits the acquired position information from the communication unit in the encrypted state (i.e., means for encrypting the present position information and means coupled to the encrypting means for sending the encrypted present position information to the central server) (see col. 6, lines 21-26).

Regarding claim 19, Giniger discloses an apparatus (see claim 17 rejection) further comprising: an acquisition unit for acquiring the position information recorded in the database, in response to a predetermined request (i.e., means for determining present position information from received position signals) (see col. 5, lines 52-53); a decryption unit for decrypting encrypted position information (i.e., means, coupled to the encrypted present position information receiving means, for decrypting the encrypted present position information) (see col. 6, lines 35-37. Also refer to col. 17, lines 29-57); a processing unit executing a predetermined process for the decrypted position information (see col. 6, lines 1-7 and lines 37-43), wherein when the decryption unit receives, together with the request, the decryption data for decrypting the encrypted position information, the decryption unit decrypts the acquired encrypted position information and transmits the decrypted position information (i.e., the mobile unit's means for

receiving response information comprises means for decrypting the encrypted response information) (see col. 6, lines 26-43). Also refer to col. 17, lines 29-57.

Although Giniger discloses a system as described, Giniger does not specifically disclose a system wherein the server, i.e., position recording apparatus, receives a key from the terminal.

However, Tatebayashi discloses a system wherein a transmission apparatus transmits a secret key (i.e., decryption key) to a receiving apparatus to decrypt received message (see abstract, col. 1, line 50-col. 2, line 11).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by Giniger with the teachings described by Tatebayashi to arrive at the claimed invention. A motivation for doing so would have been to provide secure access to information by maintaining the integrity and confidentiality of the information.

Regarding claim 20, Giniger discloses an apparatus (see claim 17 rejection) further comprising: an acquisition unit for acquiring the position information recorded in the database, in response to a predetermined request (i.e., means for determining present position information from received position signals) (see col. 5, lines 52-53); a decryption unit for decrypting encrypted position information (i.e., means, coupled to the encrypted present position information receiving means, for decrypting the encrypted present position information) (see col. 6, lines 35-37. Also refer to col. 17, lines 29-57); a processing unit for executing a predetermined process for the decrypted position information (see col. 6, lines 1-7 and lines 37-43), wherein when the decryption unit receives, together with the request, the decryption data for decrypting the encrypted position information, the decryption unit decrypts the acquired encrypted position

information and the processing unit transmits the result of the predetermined process executed for the decrypted position information (i.e., the mobile unit's means for receiving response information comprises means for decrypting the encrypted response information) (see col. 6, lines 26-43). Also refer to col. 17, lines 29-57.

Although Giniger discloses a system as described, Giniger does not specifically disclose a system wherein the server, i.e., position recording apparatus, receives a key from the terminal.

However, Tatebayashi discloses a system wherein a transmission apparatus transmits a secret key (i.e., decryption key) to a receiving apparatus to decrypt received message (see abstract, col. 1, line 50-col. 2, line 11).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by Giniger with the teachings described by Tatebayashi to arrive at the claimed invention. A motivation for doing so would have been to provide secure access to information by maintaining the integrity and confidentiality of the information.

Regarding claim 22, Giniger discloses a method of managing position information of a mobile body, comprising receiving encrypted position information relating to the position of at least one mobile body, transmitted through a radio network from a remote terminal of the mobile body (i.e., encrypting the present position information and means coupled to the encrypting means for sending the encrypted present position information to the central server) (see col. 6, lines 21-26); and recording the encrypted position information in an encrypted state, wherein the recorded encrypted position information is decrypted only after the remote terminal sends decryption data to decrypt the recorded encrypted position information and the decryption data is

received from the terminal (i.e., decrypting the encrypted present position information) (see col. 6, lines 1-7, and 26-43. Also refer to col. 17, lines 29-57).

Giniger also discloses a method wherein the position recording apparatus can decrypt the recorded encrypted position information only after the terminal sends the decryption data to allow the position recording apparatus to decrypt the encrypted position information and the position recording apparatus receives the decryption data from the terminal (i.e., means, coupled to the encrypted present position information receiving means, for decrypting the encrypted present position information) (see col. 6, lines 35-37). Also, Ginger discloses in col. 17, lines 29-57.

It should be noted that Giniger discloses a method wherein, for performing security functions, the security element utilizes an authentication and key exchange protocol, and includes, private key, public key crypto algorithm, public key certificate, symmetric key crypto algorithm (see col. 15, lines 12-18).

Giniger, however, does not specifically disclose a method wherein the recording apparatus can decrypt the previously recorded encrypted position information only after the terminal sends a key used to decrypt the previously recorded encrypted position information and that the recording apparatus receives the key from the terminal.

However, Tatebayashi discloses a method a transmission apparatus includes a secret key storage unit that stores three secret keys, a secret key selection unit that selects one secret key from the secret keys, a message generation unit for generating a message M used as a carrier for indicating a secret key, an encryption module for generating a cryptogram by encrypting the generated message using the secret key, an encryption module for generating a cryptogram by

encrypting the message using the message itself as the secret key, and two transmission units for transmitting the cryptograms to the reception apparatus to indicate the selected secret key. The reception apparatus includes a decryption module for generating decrypted data by decrypting the cryptogram using a secret key out of the three secret keys, and a decryption module for generating decrypted data by decrypting the cryptogram using the decrypted data, and authorizes that the secret key has been selected when the decrypted data matches the decrypted data (see abstract, col. 1, line 50-col. 2, line 11).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by Giniger with the teachings described by Tatebayashi to arrive at the claimed invention. A motivation for doing so would have been to provide secure access to information by maintaining the integrity and confidentiality of the information.

Regarding claim 23, Giniger discloses a method of decrypting position information of a mobile body, comprising: transmitting an encrypted position of the mobile body from to an apparatus that is separate from the mobile body (i.e., encrypting the present position information and means coupled to the encrypting means for sending the encrypted present position information to the central server) (see col. 6, lines 21-26); storing the encrypted position of the mobile body in an encrypted state in the apparatus (i.e., by receiving the present position information, the central site server inherently records or stores the present position information to compare it with stored responses information) (see col. 5, line 66 to col. 6, line 7).

Giniger does disclose a method wherein the position recording apparatus can decrypt the recorded encrypted position information (i.e., means, coupled to the encrypted present position

information receiving means, for decrypting the encrypted present position information) (see col. 6, lines 35-37). Also, Ginger discloses in col. 17, lines 29-57.

Giniger, however, does not specifically disclose a method comprising transmitting a key used for decrypting the encrypted position from the mobile body to the apparatus.

However, Tatebayashi discloses a method comprising transmitting a key used for decrypting the encrypted position from the mobile body to the apparatus (see abstract, col. 1, line 50-col. 2, line 11).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by Giniger with the teachings described by Tatebayashi to arrive at the claimed invention. A motivation for doing so would have been to provide secure access to information by maintaining the integrity and confidentiality of the information.

4. Claims 3-4, 6-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Giniger and Tatebayashi, further in view of Olsson (previously disclosed).

Regarding claim 3, the combination discloses a system as described above (see claim 1 rejection).

Although the combination discloses a system as described, the combination does not specifically disclose a system wherein upon the position recording apparatus having received a predetermined permission from a first terminal, the position recording apparatus transmits the encrypted position information, which was recorded at the position recording apparatus, of the mobile body corresponding to the first terminal, based on a request from a second terminal, and

wherein when the second terminal has directly received the decryption from the first terminal, the second terminal can decrypt the encrypted position information.

However, Olsson discloses a system wherein upon the position recording apparatus having received a predetermined permission from a first terminal, the position recording apparatus transmits the encrypted position information, which was recorded at the position recording apparatus, of the mobile body corresponding to the first terminal, based on a request from a second terminal (i.e., a client's identification information is encrypted with an encryption key previously obtained from a network location server (NLS). The encryption key may be a public key in a public key encryption system. The NLS maintains a record indicating a location associated with the identification information. The encrypted identification information is transmitted from the client to the SP. The SP launches a location request to the NLS that includes the encrypted identification information received from the client) (see paragraphs 10 and 43), and wherein when the second terminal has directly received the decryption from the first terminal, the second terminal can decrypt the encrypted position information (i.e., the MC 30 also exchanges public key(s) with the SP 60 and the SP 60 with the NLS 270) (see paragraphs 38 and 43), the second terminal can decrypt the encrypted position information (i.e., the SP 60 decrypts the location information message received from the NLS 270) (see paragraph 42).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by the references to arrive at the claimed invention. A motivation for doing so would have been to maintain the integrity and confidentiality of the location information (see paragraph 8).

Regarding claim 4, the combination discloses a system as described above (see claim 1 rejection).

Although the combination discloses a system as described, the combination does not specifically disclose a system wherein when the position recording apparatus has received predetermined permission information from the terminal, the position recording apparatus transmits the encrypted position information of a mobile body corresponding to the terminal, to a position information service center, based on a request from the position information service center providing predetermined services to the terminal, and wherein when the position information service center has received the decryption data retained by the terminal from the terminal, the position information service center decrypts the encrypted position information, executes a predetermined process for the decrypted position information and transmits the result of the process to the terminal.

However, Olsson discloses a system wherein when the position recording apparatus has received predetermined permission information from the terminal, the position recording apparatus transmits the encrypted position information of a mobile body corresponding to the terminal, to a position information service center, based on a request from the position information service center providing predetermined services to the terminal (i.e., a client's identification information is encrypted with an encryption key previously obtained from a network location server (NLS). The encryption key may be a public key in a public key encryption system. The NLS maintains a record indicating a location associated with the identification information. The encrypted identification information is transmitted from the client to the SP. The SP launches a location request to the NLS that includes the encrypted

identification information received from the client) (see paragraphs 10 and 43), and wherein when the position information service center has received the decryption data retained by the terminal from the terminal (i.e., the MC 30 also exchanges public key(s) with the SP 60 and the SP 60 with the NLS 270) (see paragraphs 38 and 43), the position information service center decrypts the encrypted position information (i.e., the SP 60 decrypts the location information message received from the NLS 270) (see paragraph 42), executes a predetermined process for the decrypted position information and transmits the result of the process to the terminal (i.e., the SP 60 then generates a service response message to the initial service request from the MC 30 with the requested service adapted to the location of the MC 30. Additionally, the SP 60 may sign the response using the SP private key. In either case, the response is encrypted using the MC public key. The MC 30 then decrypts the service response message received from the SP 60. If the SP's 60 signature is included, the MC 40 verifies the signature of the SP 60 using the SP public key. The requested service may then be presented to the subscriber via the MC 30 device, i.e., to the end-user of the device) (see paragraph 42).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by the references to arrive at the claimed invention. A motivation for doing so would have been to maintain the integrity and confidentiality of the location information (see paragraph 8).

Regarding claim 6, Giniger discloses a system (see claim 1 rejection) wherein when terminal from the terminal, the position recording apparatus, based on a request from the terminal, decrypts the encrypted position information of a mobile body corresponding to the terminal using the decryption data (see col. 6, lines 35-37. Also refer to col. 17, lines 29-57).

Although the Combination discloses a system as described, Combination does not specifically disclose a system comprising transmitting the decrypted position information to a position information service center providing predetermined services to the terminal, and wherein the position information service center executes a predetermined process for the decrypted position information and transmits the result of the process to the position recording apparatus, and wherein the position recording apparatus transmits the result of the process to the terminal.

However, Olsson discloses a system wherein the NLS decrypts the client's encrypted identification information and maintains a record indicating a location associated with the client's identification information. A SP receives the transmitted encrypted identification information from the mobile electronic equipment, transmits a location request to the NLS, the location request including the received encrypted identification information, and provides the location-based service to the subscriber via the mobile electronic equipment according to a response to the location request from the NLS (see paragraph 11).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by the references to arrive at the claimed invention. A motivation for doing so would have been to maintain the integrity and confidentiality of the location information (see paragraph 8).

Regarding claim 7, Combination discloses a system as described above (see claim 1 rejection).

Although the combination discloses a system as described, combination does not specifically disclose a system wherein when the position recording apparatus has received

predetermined permission information from the terminal, the position recording apparatus, based on a request from a third party, decrypts the encrypted position information of a mobile body corresponding to the terminal using the decryption data, executes predetermined process for the decrypted position information and transmits the result of the process to the third party.

However, Olsson discloses a system wherein when the position recording apparatus has received predetermined permission information from the terminal, the position recording apparatus, based on a request from a third party (i.e., a client's identification information is encrypted with an encryption key previously obtained from a network location server (NLS). The encryption key may be a public key in a public key encryption system. The NLS maintains a record indicating a location associated with the identification information. The encrypted identification information is transmitted from the client to the SP. The SP launches a location request to the NLS that includes the encrypted identification information received from the client) (see paragraphs 10-13, and 43), decrypts the encrypted position information of a mobile body corresponding to the terminal using the decryption data (i.e., the NLS decrypts the client's encrypted identification information and maintains a record indicating a location associated with the client's identification information) (see paragraphs 10-13), executes predetermined process for the decrypted position information (i.e., maintains a record indicating a location associated with the client's identification information) (see paragraphs 10-13), and transmits the result of the process to the third party (i.e., SP receives the transmitted encrypted identification) (see paragraphs 10-13).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by the references to arrive at the claimed

invention. A motivation for doing so would have been to maintain the integrity and confidentiality of the location information (see paragraph 8).

Regarding claims 8-9, the combination discloses a system (see claim 7 rejection) wherein the predetermined process is a process for responding to a query relating to a mobile body corresponding to the terminal (i.e., sending a retrieved response to the mobile terminal) (see col. 6, lines 37-43).

Regarding claim 10, Giniger discloses a system (see claim 7 rejection) wherein the query is at least one of "where is the current position of the mobile body", "whether the mobile body is/was at a designated place", "whether the mobile body is/was at a designated place on a designated date at a designated time", "where is the position at which the mobile body was on a designated date at a designated time" and "on which data and at what time the mobile body was at a designated place" (i.e., from the request, the central site server may correct the motion of the mobile user if the user is going in the wrong direction (e.g., request and response related to the current position of the mobile body) (see col. 11, lines 21-32).

5. Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Giniger and Tatebayashi, further in view of Pirila, U.S. Patent No. 6674860.

Regarding claim 11, the combination discloses a system as described (see claim 1 rejection).

Although the combination discloses a system as described, the combination does not specifically disclose a system wherein the terminal comprises a plurality of encryption means, and is capable of switching the encryption means for encrypting the position information, based

on the position of the terminal and/or the time, or on an instruction from a mobile body (i.e., the decryption key can be changed, in which case the new decryption key is transferred to the mobile station advantageously periodically in conjunction with the location update procedure) (see abstract).

However, Pirila discloses a system wherein the terminal comprises a plurality of encryption means, and is capable of switching the encryption means for encrypting the position information, based on the position of the terminal and/or the time, or on an instruction from a mobile body (i.e., the decryption key can be changed, in which case the new decryption key is transferred to the mobile station advantageously periodically in conjunction with the location update procedure) (see abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described to arrive at the claimed invention. A motivation for doing so would have been to ensure the security as related to the transmission of the location information.

Regarding claim 12, Giniger discloses a system (see claim 1 rejection) wherein the terminal the terminal can measure the position of the mobile body (i.e., means for determining present position information from received position signals) (see col. 5, lines 52-53), encrypt the measured position information with predetermined encryption means and transmit the encrypted position information (i.e., means for encrypting the present position information and means, coupled to the encrypting means, for sending the encrypted present position information to the central server) (see col. 6, lines 21-26).

Although the combination discloses a terminal as described, the combination does not specifically disclose that the terminal comprises a personal authentication means for a mobile body, and wherein when a personal authentication is successfully completed, the terminal can measure the position of the mobile body.

However, Pirila discloses a system wherein the terminal comprises a personal authentication means for a mobile body (i.e., SIM module) (see fig. 10, col. 8, lines 48-49), and wherein when a personal authentication is successfully completed, the terminal can measure the position of the mobile body (i.e., SIM module manages the data required for the identification of the subscriber) (see abstract and col. 8, lines 65-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings to arrive at the claimed invention. A motivation for doing so would have been to ensure the security as related to the transmission of the location information.

6. Claims 13-14, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Giniger and Tatebayashi, further in view of Walsh (previously disclosed).

Regarding claims 13 and 20, Giniger discloses a system (see claims 1 and 20 rejections) wherein the position recording apparatus receives the decryption data from the terminal and decrypts the encrypted position information using the decryption data (i.e., means, coupled to the encrypted present position information receiving means, for decrypting the encrypted present position information) (see col. 6, lines 35-37. Also refer to col. 17, lines 29-57).

Although the combination discloses a system as described, the combination does not specifically disclose a system wherein the position recording apparatus stores in a temporary

memory the decryption data, the decrypted position information and the result of a predetermined process executed for the decrypted position information and erases (i.e., erasing unit) from the temporary memory the decryption data, the decrypted position information and the result of the process after transmitting the result of the process to the terminal.

However, Walsh discloses a system wherein the position recording apparatus stores in a temporary memory the decryption data, the decrypted position information and the result of a predetermined process executed for the decrypted position information and erases from the temporary memory the decryption data, the decrypted position information and the result of the process after transmitting the result of the process to the terminal (i.e., the location-enabled service 108 stores the location information in the location-enabled service. The storage is relatively temporary, until the location-enabled service 108 receives updated location information from the wireless communication device 104) (see paragraph 132).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described to arrive at the claimed invention. A motivation for doing so would have been to ensure that updated location information as related to the present position of the terminal is being maintained.

Regarding claim 14, Giniger discloses a system (see claim 13 rejection) wherein the position recording apparatus executes the predetermined process (i.e., the central site server's means for sending the retrieved response information to the mobile unit comprises means for encrypting the retrieved response information; and means, coupled to the retrieved response information encrypting means, for sending the encrypted retrieved response information to the mobile unit via the bidirectional communications link) (see col. 6, lines 37-43).

7. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Giniger, Tatebayashi, and Walsh, further in view of Olsson.

The combination discloses a system as described above (see claim 13 rejection).

Although the combination discloses a system as described, the combination does not specifically disclose a system wherein system wherein the position recording apparatus transmits the decrypted position information to a position information service center providing predetermined services utilizing the position information and receives from the position information service center the result of the predetermined process executed by the position information service center.

However Olsson discloses a system wherein the position recording apparatus transmits the decrypted position information to a position information service center providing predetermined services utilizing the position information (i.e., a client's identification information is encrypted with an encryption key previously obtained from a network location server (NLS). The encryption key may be a public key in a public key encryption system. The NLS maintains a record indicating a location associated with the identification information. The encrypted identification information is transmitted from the client to the SP. The SP launches a location request to the NLS that includes the encrypted identification information received from the client) (see paragraphs 10 and 43) and receives from the position information service center the result of the predetermined process executed by the position information service center (i.e., the NLS decrypts the client's encrypted identification information and maintains a record indicating a location associated with the client's identification information. A SP receives the

transmitted encrypted identification information from the mobile electronic equipment, transmits a location request to the NLS, the location request including the received encrypted identification information, and provides the location-based service to the subscriber via the mobile electronic equipment according to a response to the location request from the NLS) (see paragraph 11).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings as described by the references to arrive at the claimed invention. A motivation for doing so would have been to maintain the integrity and confidentiality of the location information (see paragraph 8).

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PIERRE-LOUIS DESIR whose telephone number is (571)272-7799. The examiner can normally be reached on Monday-Friday 9:00AM- 5:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dwayne Bost can be reached on (571)272-7023. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Pierre-Louis Desir/
Examiner, Art Unit 2617

/Dwayne D. Bost/
Supervisory Patent Examiner,
Art Unit 2617